WHAT IS CLAIMED IS:

1. A device for providing a user with secure access to a network resource, comprising:

a first module for authenticating a user to said device;

a second module responsive to said first module for providing the user with access to the network resource using a network resource password unknown to the user.

2. The device of claim 1 wherein the first module uses one or more of the following to authenticate the user to the device: a user password entered by the user, user biometrics and possession of the device.

3. The device of claim 2 further comprising an accounts database for storing information regarding the network resources accessible to an authenticated user.

4. The device of claim 2 wherein the first module is responsive to a user password or a duress password for authenticating a user to the device.

5. The device of claim 4 including a duress database and an accounts database, wherein entry of a correct duress password to authenticate to the device permits user access only to network resources set forth in said duress database, and wherein entry of a correct user password to authenticate to the device permits access to only network resources set forth in said accounts database.

6. The device of claim 5 wherein the network resources set forth in the duress database are those network resources not containing sensitive information, and wherein the network resources set forth in the accounts database are those to which the user would like to deny access by unauthorized users.

7. The device of claim 2 wherein the device further comprises a biometrics database for storing biometrics of authorized device users.

8. The device of claim 7 wherein the first module is responsive to user biometrics for authenticating the user to the device, wherein the biometrics are compared with biometrics in the biometrics database, wherein the user is authenticated to the device if the user biometrics are determined to match biometrics in the biometrics database.

9. The device of claim 8 wherein the biometrics are selected from among: a fingerprint, a retina scan, a written word, a plurality of written words, and a signature.

10. The device of claim 2 wherein the first module is responsive to the concurrent entry of biometrics and the user password.

11. The device of claim 10 wherein the device further comprises an entry pad onto which the user inscribes the user password, and wherein the biometrics comprise the characteristics of the inscribed user password.

12. The device of claim 2 wherein the device further comprises a user password database for storing user passwords of authorized users.

13. The device of claim 12 wherein the first module is responsive to a user entered password, wherein the entered user password is compared with user passwords stored in the user password database for determining whether the user is an authorized user.

14. The device of claim 1 further comprising an accounts database for storing network resources information, wherein an authenticated user has access to network resources stored in said accounts database, and wherein the second module is responsive to said accounts database for use in accessing the network resource.

15. The device of claim 14 wherein the access information for each network resource includes the network resource address, the network resource user identification, and the network resource password.

16. The device of claim 15 wherein the network resource password is generated using random numbers.

17. The device of claim 16 further comprising an entropy pool including a plurality of random numbers for use in generating the network resource password.

18. The device of claim 15 wherein the network resource password is modified on a predetermined schedule.

19. The device of claim 15 wherein the network resource password is modified each time access is gained to the network resource.

20. The device of claim 1 further comprising a communications module for transferring data in encrypted form over a communications link between the device and the network resource.

21. The device of claim 20 wherein the communications link is chosen from among: a radio frequency link, an optical link, and an infrared link.

22. The device of claim 20 wherein the communications link comprises the Internet.

23. The device of claim 1 wherein a computer is interposed between the device and the network resource, wherein certain information transferred between the device and the network resource is displayed on the computer, and wherein certain other information transferred between the device and the network resource is in encrypted form and is not displayed on the computer.

24. The device of claim 1 further comprising a magnetic code writing module, wherein when a user is authenticated to the device, the device is operative to write information to a magnetic strip.

25. The device of claim 24 wherein the information written to the magnetic strip includes credit card information and wherein the magnetic strip is affixed to a plastic substrate, and wherein when the account information is written to the magnetic strip, a credit card is formed.

26. The device of claim 1 wherein the device size permits hand-held operation of the device.

27. The device of claim 1 wherein the second module logs the device onto the network resource by contacting the network resource and providing the required log-on information without intervention by the user.

28. The device of claim 27 wherein the log-on information includes the network resource password and wherein the network resource password is created by a random process without intervention by the user.

29. The device of claim 1 further comprising input modules selected from among: a microphone, a touch-sensitive display screen, a keyboard, and a camera.

30. The device of claim 1 further comprising output modules selected from among: a speaker, a display, and a printer.

31. The device of claim 1 wherein a plurality of users are authorized to use a specific device, and wherein the device further comprises an accounts database designating the accounts to which each user has access, a user password database including the user password for each authorized user, and a biometrics database

including the biometrics for each authorized user, and wherein the first module is responsive to the user-entered user password and biometrics for comparing the contents of said user password database and said biometrics database for determining if the user is an authorized user, and in response thereto, authenticating the user to the device, thereby permitting the user to access the designated accounts in the accounts database.

32. The device of claim 1 further comprising a preferences database for storing device operational parameters for the authorized user.

33. The device of claim 32 wherein the device operational parameters include the conditions for changing the network resource password.

34. The device of claim 32 wherein after the user is authenticated to the device, the user can change the preferences stored in the preferences database.

35. The device of claim 1 further comprising a device dependent key, wherein the contents of the first and the second module are stored in encrypted form and wherein said device dependent key is required to decrypt the contents of the first and the second modules.

36. The device of claim 35 wherein the contents of the first and the second module are backed up in encrypted form from the device to a storage module, wherein the device dependent key is not backed up to said storage module, such that the contents of the first and the second module as stored in said storage module cannot be decrypted.

37. The device of claim 1 further comprising hardware and software elements for performing functions unrelated to accessing a network resource.

38. The device of claim 1 further comprising a document storage module for storing documents intended for execution by the user, wherein upon authentication to the device, the user retrieves a document from said document storage module and electronically executes the document.

39. The device of claim 1 wherein a document is downloaded from the network resource to the device after the user is authenticated, and wherein the user electronically executes the document and returns the document to the network resource.

40. The device of claim 1 wherein the network resource is an appliance and wherein after the user is authenticated to the device, the device, under user control, communicates with the appliance.

41. The device of claim 40 wherein the device communicates with the appliance by sending a signal for controlling the appliance.

42. The device of claim 40 wherein after the user is authenticated to the device, the device is operative to send a signal to a computer, and wherein in response to said signal, the computer controls the appliance.

43. A method for authenticating a user to a device for contacting a network resource, said method comprising the steps of:

(a) a user providing a user password;

(b) a user providing biometrics;

(c) determining if the user password and the user biometrics match the password and the biometrics of an authorized user;

(d) retrieving from device memory a randomly generated password for the network resource; and

(e) transmitting the randomly generated password to the network resource to gain access thereto.

44. The method of claim 43 wherein the device includes an accounts database for storing information required to gain access to the network resource, further comprising a step (f) adding a network resource to the accounts database.

45. The method of claim 44 wherein the step (f) further comprises:

(f1) accessing the network resource;

(f2) receiving from the network resource a template for providing network resource access parameters required to gain access to the network resource;

(f3) providing at least one dummy network resource access parameter and any additional required network resource access parameters to the network resource;

(f4) storing the network resource template; and

(f5) changing the at least one dummy network resource access parameter when the network resource is next accessed.

46. The method of claim 45 further comprising a step (f6) on a predetermined schedule, changing the randomly generated password for the network resource.

47. The method of claim 43 wherein the step (e) further comprises transmitting the randomly generated password in encrypted form.

48. A method for authenticating to a device for accessing a network resource, wherein certain operational code or data of the device is stored in encrypted form, and wherein the device includes a device dependent key, said method comprising the steps of:

(a) a user providing a user password;

(b) a user providing biometrics;

(c) determining if the user password and the user biometrics match the password and the biometrics of an authorized user;

(d) using the device dependent key, decrypting the certain operational code or data stored in encrypted form;

(e) retrieving from the device memory the randomly generated password for the network resource; and

(f) transmitting the randomly generated password to the network resource to gain access thereto.

49. An article of manufacture comprising:

a computer program product comprising a computer-usable medium having a computer-readable code therein for authenticating a user to a device for contacting a network resource, the computer-readable code in the article of manufacture comprising:

a computer-readable program code module for receiving a user password;

a computer-readable program code module for receiving biometrics;

a computer-readable program code module for determining if the user password and the user biometrics match the password and the biometrics of an authorized user;

a computer-readable program code module for retrieving a randomly generated password for the network resource; and

a computer-readable program code module for transmitting the randomly generated password to the network resource to gain access thereto.